Kurzprotokoll der 6. Sitzung der IuK-Kommission
Kommission des Ältestenrates für den Einsatz neuer Informations- und Kommunikationstechniken und -medien

Berlin, den 21. Mai 2015, 8:00 Uhr
Sitzungsort: 10557 Berlin, Friedrich-Ebert-Platz 1
Sitzungssaal: Plenarbereich Reichstagsgebäude, Ältestenratssaal (Raum 2 N014)

Vorsitz: VPn Petra Pau, MdB

Leaked 10 June 2015 by BILD, highlights and translations by Thomas Rid

Die **Vorsitzende** begrüßt die Teilnehmer zur außerordentlichen Beratung der IuK-Kommission. Aus persönlichen Gründen sei es nicht möglich gewesen, vor der heutigen Beratung eine Besprechung der Obleute einzuberufen. Die **Vorsitzende** führt kurz in den Sachverhalt des Angriffes auf die Informationstechnik des Deutschen Bundestages ein und übergibt zur Darstellung der Sicht der Bundestagsverwaltung Herrn Möhlmann (RL IT 5) das Wort.

Tagesordnungspunkt 1

Bericht des BSI-Präsidenten, Herrn Hange, zum Angriff auf die IT des Deutschen Bundestages

Herr Möhlmann (RL IT 5) erläutert, dass am 8.5.2015 im Rahmen der normalen Betriebsüberwachung festgestellt worden sei, dass zwischen Serversystemen nicht übliche Kommunikation stattgefunden habe. Konkret sei ein Server der Bundestagsverwaltung in einem Festplattenbereich mit einer ungewöhnlichen Menge an Daten überlastet worden. In einer darauf folgenden Analyse der Kommunikationsbeziehungen sei festgestellt worden, dass zu diesem Server nicht vorgesehene Verbindungen von einem Abgeordnetenbüro bestanden haben. **Herr Möhlmann (RL IT 5)** weist darauf hin, dass es sich zunächst um Untersuchungen im Rahmen des Alltäglichen gehandelt habe, da im Haus häufiger Trojaner und Viren gefunden und dann nach festgelegten Regeln beseitigt würden. Daher seien kurzfristig die betroffenen Rechner ausgetauscht und durch neue Rechner ersetzt worden. In der weiteren Analyse sei ermittelt worden, dass von den Rechnern des Abgeordnetenbüros zusätzlich eine Verbindung zu einem Server einer Fraktion bestanden habe. **Herr Möhlmann (RL IT 5)** führt aus, dass in Zusammenarbeit mit der betroffenen Fraktion weiter festgestellt worden sei, dass auf diesen Server auch von einem Rechner eines Abgeordnetenbüros der eigenen Fraktion ein Zugriff in unüblicher Form stattgefunden habe.
Im weiteren Verlauf der Überprüfung sei dann festgestellt worden, dass Accounts von Administratoren – ohne Wissen der Accountinhaber – genutzt worden seien.
Herr Möhlmann (RL IT 5) teilt mit, dass sich am 12.5.2015 das Bundesamt für Verfassungsschutz (BfV) mit der Geheimschutzstelle (ZR 4) der Bundestagsverwaltung in Verbindung gesetzt habe. Das Referat ZR 4 habe daraufhin das Referat für IT-Sicherheit (IT 5) kontaktiert. In einem anschließenden Telefonat sei durch einen Mitarbeiter des BfV mitgeteilt worden, dass zwei Rechner aus dem Bundestag Kontakt zu – als potentiell gefährlich geltenden – Serversystemen im Internet gehabt haben und das BSI darüber in Kenntnis gesetzt worden sei. Es sei weiterhin durch die BTV festgestellt worden, dass diese gemeldeten Rechner identisch gewesen seien mit zuvor im Haus auffällig gewordenen PCs. Ob der Dimension des vermuteten Angriffes sei das Bundesamt für Sicherheit in der Informationstechnik (BSI) um Hilfe ersucht worden. Am 15.5.2015 seien zusammen mit dem BSI umfangreiche Analysetätigkeiten begonnen worden.
Die **Vorsitzende** übergibt Herrn Hange (BSI) das Wort.
Herr Hange (BSI) bemerkt, dass aus technischer Sicht Cyberangriffe aktuell keine Besonderheit seien, sich jedoch stark in der Qualität unterschieden.
Er berichtet von ca. 3000 Angriffen auf das Regierungsnetz, von denen ca. 5 bis 10 von einer zum beobachteten Angriff vergleichbaren Qualität seien. Aus Erfahrung des BSI seien auch sehr viele Firmen von regelmäßigen Angriffen in vergleichbarem Ausmaß betroffen. Die Auswertungen haben bislang ergeben, dass es dem Angreifer gelungen sei, Administrationsrechte für die gesamte Infrastruktur zu erhalten. Daher sei von einer breiten Kompromittierung der Netzinfrastruktur mit höchstmöglichen Rechten auszugehen. Hinweisen auf die gezielte Verwendung eines hoch-qualifizierten Anwendungsprogramms werde aktuell noch nachgegangen. Man befände sich im Moment in der ersten Phase der technischen Analyse. Nach Beurteilung der Lage hätten ab Samstag, dem 16.05.2015 insgesamt drei Mitarbeiter des BSI und zwei Mitarbeiter einer externen Firma, mit der das BSI seit Längerem zusammenarbeite, die Analysetätigkeit aufgenommen. Gerade die erste Phase einer Ermittlung sei wichtig, da der Täter meist noch nicht erahne, dass man ihm auf der Spur sei. Ziel dieser Phase sei es, möglichst viele Nachweise zu finden, um das Angriffsmuster zu erkennen. Durch die Besonderheit der Netzinfrastruktur des Bundestages sei eine enge Zusammenarbeit mit den IT-Experten der Verwaltung unabdingbar.
Herr Hange (BSI) weist auf fehlerhafte Pressemeldungen hin, nach denen es sich um einen DDoS-Angriff handeln solle. Auch gäbe es keinerlei konkrete Hinweise darauf, dass Daten des NSA-Untersuchungsausschusses abgeflossen seien. Er betont jedoch, dass man dieses zurzeit aber auch nicht

BSI reports 3K attacks on gov networks, only 5 to 10 of comparable quality

The analysis of the current breach started on 16 May. 3 BSI staff and 2 contractors from an "external company" worked on the case. The company played a key role, it seems, but is not named in this report. Why is unclear.

Correction: The company is BFK edv-consulting GmbH, see below. (via @ochsff, thanks @empiricalerror)

ausschließen könne. Durch die Tatsache, dass man am Internet teilhabe, seien Informationsflüsse nach außen nicht grundsätzlich auszuschließen. Zu beobachten sei bislang ein unterbundener Versuch eines Informationsabflusses.

In Zusammenarbeit mit der IT des Bundestages seien nun folgende Maßnahmen ergriffen worden: Zunächst würden möglichst viele Internetzugriffe über den IVBB geleitet, in dem ein Mechanismus greife, welcher ca. 100.000 Server und Netze als potentiell gefährlich kenne und den Zugriff darauf blocke. Die eingangs genannten Zielserver seien in diesem Filter bereits bekannt gewesen. Somit könne in einem ersten Schritt verhindert werden, dass dorthin weitere Daten abflössen. Der Zugriff auf die als kritisch bekannten Seiten werde hierbei blockiert.

Herr Hange (BSI) berichtet, dass im weiteren Schritt Logdaten analysiert und die Protokollierungsdauer in Abstimmung mit dem Bundestag erweitert worden sei. Ein Problem für die Analyse sei es, wenn der Ursprung eines Angriffes aufgrund fehlender Protokolldaten nicht nachvollzogen werden könne. Beispielsweise sei der erste Einbruch auf die französische Senderkette TV5Monde zwei Monate vor Entdeckung des Angriffes erfolgt. Dieses könne nur über eine umfangreiche Protokollierung nachvollzogen werden.

Im Einsatz seien vonseiten des BSI nun auch Experten, welche auch den IVBB schützten. Diese Forensiker setzten nun aus beobachteten Phänomenen ein Bild zusammen, um Ursachen und weitere Maßnahmen zu ermitteln. Auch seien bereits Endsysteme neu aufgesetzt worden, die als befallen identifiziert werden konnten.

Der Nachweis und die Analyse seien durch die Beschränkung auf sieben Tage Protokollierung sehr ambitioniert. Angriffe dieser Qualität seien in Pakete aufgeteilt, welche einzeln harmlos aussähen. Erst in einer gesamten Kette betrachtet sei zu erkennen, was wirklich passiere.

Herr Hange (BSI) betont noch einmal, dass man nach den aktuell vorliegenden Erkenntnissen davon ausgehen müsse, dass das Netz großflächig und umfangreich kompromittiert sei. Schutzmaßnahmen griffen z. B. nur noch eingeschränkt. Eine absolute Sicherheit hinsichtlich Informationsabfluss könne daher nicht garantiert werden. Es seien weitere Analysen notwendig, um zu entscheiden, ob durch Neuinstallation einzelner betroffener Systeme, von Teilen der Infrastruktur oder des Gesamtnetzes eine wirksame Bereinigung des Gesamtsystems erreicht werden könne.

Grob könne der Ablauf in drei Phasen aufgeteilt werden: In der ersten Phase werde eine technische Analyse erstellt. Diese brauche erfahrungsgemäß Zeit, da der analytische Aufwand sehr hoch sei. In einer zweiten Phase sei geplant, den Täter in seinen Möglichkeiten zu behindern und einzugrenzen und befallene Systeme zu bereinigen. In der dritten Phase sei dann die Neuinstallation von Teilen des Systems oder des Gesamtsystems geplant.

Response in phases:

1: technical analysis, very labour intensive

2: start making exploitation difficult for adversary

3: clean-up, re-install parts of the system or all of it

Die **Vorsitzende** erteilt dem Abg. Dr. Brandl das Wort für Nachfragen.

Abg. Dr. Brandl zeigt Verständnis für die eingeschränkte Kommunikation in dieser Situation, um den Tätern keine Hinweise zu geben. Er bemängelt jedoch kommunikative Defizite am Freitag, dem 15.5.2015, an dem alle Rechner im Bundestag heruntergefahren worden seien. Der kurze und einzige Hinweis, dass der Rechner in einer Minute heruntergefahren werde, sei nicht ausreichend. Eine Vorwarnung in solchen Fällen, etwa von 5 Minuten, sei wünschenswert.

Er bemängelt weiterhin eine nicht ausreichende Information der Mitglieder der IuK-Kommission. Er habe bis zur heutigen Sitzung alle Informationen nur der Presse entnommen. Er verweist darauf, dass der Entschluss zur Reduktion der Protokollierung auf sieben Tage sicher gute Gründe gehabt habe, dass man aber auch darstellen sollte, welche Analysemöglichkeiten im Falle eines solchen Angriffes dadurch verloren gingen.

BSI reports TV5 attack in France started two months before discovery.

Die **Vorsitzende** erteilt der Abg. Dr. Sitte das Wort.

Abg. Dr. Sitte bestätigt, dass auch aus ihrer Sicht die Kommunikation schwierig gewesen sei. Sie regt an, sich in diesem Gremium über die erforderlichen und angemessenen Kommunikationsschritte zu einigen. Eine zeitnahe Information der Mitglieder des Deutschen Bundestages halte sie für dringend geboten, um der Gerüchteküche entgegentreten zu können. Dieses sei auch sinnvoll, um eine einheitliche Informationspolitik gegenüber Vertretern der Medien zu ermöglichen. Sie betont, dass es gerade in dieser ersten Phase der Analyse hilfreich sei, in eine geregelte und regelmäßige interne Kommunikation einzutreten.

Sie führt aus, dass einer der bisher betroffenen Rechner sich in einem Abgeordnetenbüro ihrer Fraktion befände. Es seien bereits vor dem dokumentierten Fund aus dem betreffenden Abgeordnetenbüro Auffälligkeiten vermeldet worden. Diese hätten allerdings nicht auf ein solches Ereignis hingedeutet. Den weiteren Verlauf der Ereignisse könne sie bestätigen. Die Abgeordnete fragt, ob

Fremdgeräte eine physische Verbindung zum Bundestagsnetz gehabt hätten. Zusätzlich bittet sie um Erläuterung, ob bereits Erkenntnisse vorlägen, um welche Schadsoftware es sich handele und ob ein Programm oder mehrere verantwortlich seien. Weiter möchte sie wissen, ob es sich bei der Software um eine spezielle Version für den Bundestag handele oder ob diese bereits früher beobachtet worden sei. Sie bittet zudem um Informationen, über welches Schadpotential das Programm verfüge und welchen Funktionsumfang es habe. Des Weiteren fragt **Abg. Dr. Sitte**, ob der Angriff noch andauere und bittet um Informationen, welche Planungen es bereits für eine Bereinigung des Gesamtsystems gäbe.

Abg. Klingbeil erläutert, dass er im Kollegenkreis ein gewisses Maß an Verunsicherung registriert habe. Er bittet Herrn Hange (BSI) um nähere Erläuterung, ob es im Zusammenhang mit dem NSA-Untersuchungsausschuss Hinweise gäbe, dass ein Datenabfluss stattgefunden habe. Er stellt ebenfalls die Frage, um welche Art von Firma es sich handele und worin deren spezielle Expertise bestehe, die im BSI offensichtlich nicht vorhanden sei. Ferner möchte er wissen, ob es Erkenntnisse über den Zeitpunkt des ersten Zugriffs gäbe. Er bittet um eine detailliertere Erläuterung, wie es zur Entdeckung des Angriffes gekommen sei und wie der von Abg. Dr. Sitte angesprochene Fall zu bewerten sei. Er fragt, ob es theoretisch vorstellbar sei, dass der Angriff seit einem Jahr andauere, ohne entdeckt worden zu sein. Im Weiteren bittet er um Aufklärung, wie der Verfassungsschutz parallel zu den Erkenntnissen gekommen sei und welcher Art diese Hinweise seien. Er bittet um Aufklärung, was unter der Formulierung „Umfassend kompromittiert" im Bericht von Herrn Hange (BSI) zu verstehen sei. Darüber hinaus bittet er um eine Erläuterung zu der Meldung, dass ein Geheimdienst in den Angriff involviert sei und wie ein Zeitplan zur Bewältigung der Krise aussähe.

Abg. Lemke bestätigt die Einschätzung, dass dieser Angriff als sehr ernst einzustufen sei. Sie lobe ausdrücklich die Kommunikation vonseiten der Bundestagsverwaltung. Sie werde sich nicht an den naheliegenden Spekulationen zu den Quellen der in den Medien kursierenden Gerüchten beteiligen. Allerdings seien in einem Artikel sogenannte Sicherheitskreise zitiert worden. Da diese weder die Bundestagsverwaltung noch der Bundestag sein könne, stelle sich die Frage, inwieweit Herr Hange (BSI) das Kommunikationsverhalten seiner Mitarbeiter und der beteiligten Firma im Griff habe. Sie regt daher an, die Informationen zuerst an die Mitglieder des Deutschen Bundestages zu geben, bevor die Presse informiert werde. Eine andere Vorgehensweise halte sie für nicht akzeptabel. Sie sei zudem sehr daran interessiert, dass das in diesem Vorgang vorhandene Leck aufgedeckt werde. Sie bittet um eine Erläuterung, wie und in welcher Form der Verfassungsschutz am 12.5.2015 bemerkt habe, dass Rechner des Bundestages auffällig geworden seien.

Des Weiteren interessiere sie sich dafür, wie die Zusammenarbeit zwischen Bundestagsverwaltung und BSI organisiert sei und für Art, Umfang und Rolle der Unterstützung des BSI durch eine externe Firma. Sie fragt außerdem nach den personellen Ressourcen, die vonseiten des BSI zur Verfügung gestellt würden und wie die Aussage, dass die Sicherheit nicht garantiert werden könne, zu verstehen sei. Weiter regt sie an, die Mitglieder des Deutschen Bundestages entsprechend zu informieren.

Die Vorsitzende erläutert, dass verschiedene Fachausschüsse Interesse bekundet hätten, sich mit dem Thema zu beschäftigen. In Absprache mit den Ausschussvorsitzenden und den Fraktionen sei vereinbart worden, dass die Fachausschüsse die jeweiligen Berichtsanträge zurückstellen und die IuK-Kommission das aktuell erste und einzige Gremium sei, das sich mit dem Angriff befasse. Sie schlägt vor, dass die Fragen zunächst, soweit möglich, von Herrn Möhlmann beantwortet würden und Herr Hange anschließend die Antworten ergänze.

Herr Möhlmann (RL IT 5) stimmt den von Abg. Dr. Brandl festgestellten Einlassungen zu. Er teilt mit, dass es sich beim angesprochenen Herunterfahren der Rechner um eine in der UA IT abgestimmte Maßnahme gehandelt habe und zunächst geprüft worden sei, wann diese möglichst störungsarm durchgeführt werden könnte. Weiterhin führt er aus, dass es schwierig gewesen sei, zu diesem Zeitpunkt noch alle Betroffenen zu erreichen und dass eine E-Mail-Information als nicht unbedingt zielführend angesehen worden sei.

Auf die Frage der **Abg. Dr. Sitte** nach dem Zusammenhang mit einem Rechner einer Abgeordneten und einem Server ihrer Fraktion teilt **Herr Möhlmann (RL IT 5)** mit, dass die Bundestagsverwaltung dazu keine Auskunft geben könne und dies mit der betreffenden Fraktion diskutiert worden sei. **Abg. Dr. Sitte** wirft korrigierend ein, dass sie klären wolle, warum die IT nicht bereits tätig geworden sei, als das Abgeordnetenbüro sich wegen Auffälligkeiten schon zuvor an die IT gewandt

Lars Klingbeil (SPD) is asking sharp questions.

What company?

What can they do that BSI can't?

When did the breach begin?

habe. **Herr Möhlmann (RL IT 5)** stellt klar, dass er hiervon keine Kenntnis bekommen habe und der Angriff genauso aufgefallen sei, wie er es dargestellt habe.
Auf die Frage bezüglich Fremdgeräten antwortet **Herr Möhlmann (RL IT 5)**, dass sich ausschließlich Parlakom-Geräte und selbstverständlich Fraktionsgeräte im Netz befänden. Fremdgeräte im Sinne von Geräten, die nicht in das Bundestagsnetz gehörten, gäbe es daher nicht.
Abg. Dr. Sitte stellt klar, dass sie dies wisse und es ihr darum ginge, ob aufgrund der Schadsoftware der Zugriff von Fremdgeräten möglich gewesen sei oder ob dies ausgeschlossen werden könne.
Herr Möhlmann (RL IT 5) verweist bzgl. der Fragen zu den speziellen Schadprogrammen auf Herrn Hange (BSI).
Abg. Klingbeil möchte wissen, seit wann der Angriff bekannt sei.
Herr Möhlmann (RL IT 5) informiert, dass am 8.5.2015 die Mitarbeiter der Unterabteilung IT Unregelmäßigkeiten festgestellt haben, die zu diesem Zeitpunkt noch nicht als Angriff gewertet worden seien, sondern als alltäglicher Fall im Zusammenhang mit Viren und Trojanern. Erst das Gespräch mit dem BfV am 12.5.2015 habe verdeutlicht, dass es sich um einen Angriff handele. Das BfV hätte deutlich gemacht, dass der Zugriff von zwei Rechnern aus dem Bundestag festgestellt worden sei. Diese Rechner seien namentlich benannt worden und hätten somit als Bundestagsrechner identifiziert werden können. In diesem Gespräch sei auch mitgeteilt worden, dass das BSI seitens des Verfassungsschutzes informiert werde, speziell das Cyberabwehrzentrum.
Abg. Lemke erkundigt sich, was genau der Verfassungsschutz festgestellt habe.
Herr Möhlmann (RL IT 5) führt aus, dass ihm telefonisch mitgeteilt worden sei, dass von zwei Rechnern aus dem Bundestagsnetz auf kompromittierte Seiten, die überwacht worden seien, ein Zugriff stattgefunden habe. Er erklärt, dass kompromittierte Seiten z. B. sog. Command-and-Control-Server seien, die im Internet existierten, um Malware zu verteilen und auch „Angriffssoftware" enthielten.
Herr Häger (BSI) führt ergänzend aus, dass das BfV diese speziellen Informationen von einer Firma bekommen habe, welche von einem anderen Land beauftragt worden und an die Verschwiegenheit gebunden sei. Dieses Land habe jedoch zugestimmt, dass der von der beauftragten Firma ermittelte Hinweis weitergegeben werden dürfe.

Herr Hange (BSI) stellt klar, dass das BSI nur für die technische Analyse zuständig sei und in diesem Zusammenhang auch Server im Internet feststelle, die Schadprogramme verteilen oder für Informationsabfluss genutzt werden. Für das Regierungsnetz seien viele solcher kritischen Server gelistet und so auch der Server, mit dem der Bundestagsrechner in Kontakt stand. Er betont dass es keine Überwachungsmaßnahme des Bundestages gewesen sei, sondern es sich um einen Zufallsfund gehandelt habe. Aufgrund der technischen Zuständigkeit sei dann das BSI vom BfV informiert worden, weil auch die Bundesregierung hätte betroffen sein können. Das BSI übernehme grundsätzlich eine beratende Funktion beim Bundestag. Die Koordination der aktuellen Maßnahmen läge ausschließlich beim Bundestag. Herr Dr. Winterstein habe aufgrund der Schwere des Angriffes alle verfügbaren Experten zur Aufklärung des Sachverhaltes angefordert.
Abg. Lemke erkundigt sich, wer die Erlaubnis erteilt habe.
Herr Hange (BSI) stellt klar, dass das BSI keine nachrichtendienstlichen Beobachtungen durchführe und schlägt vor, beim BfV zuständigkeitshalber nachzufragen, da das BSI auch nur Empfänger der Information gewesen sei.
Er betont, dass es wichtig sei, bei der Analyse schnell zu handeln. Daher sei am Freitag mit der Voruntersuchung begonnen und dann entschieden worden, massiv in die Untersuchung einzusteigen. Er führt aus, dass Spuren schnell verloren gehen könnten, wenn nicht kompakt eingegriffen würde. Es habe bislang festgestellt werden können, dass aktuell nur wenige Endsysteme betroffen seien. Die Angreifer seien jedoch so tief in das Netz eingedrungen, dass sie jederzeit wieder aktiv werden könnten. Momentan würde nun versucht, die Wege nach außen zu blockieren und dem Angreifer das Agieren so schwer wie möglich zu machen. Es handele sich um ein auch an anderer Stelle bereits verwendetes und öffentlich bekanntes Angriffsmuster, sodass noch keine Rückschlüsse auf die Täter gezogen werden könnten. Professionelle Angreifer bedienten sich häufig verschiedener Angriffsmuster, um falsche Fährten zu legen, was einen Rückschluss auf die Täter erschweren solle.
Herr Hange (BSI) versichert, dass das BSI nicht von sich aus die Öffentlichkeit informiere. Es sei vielmehr üblich, dass das BSI den jeweils Betroffenen unterrichte und dieser dann entscheiden könne, ob die Öffentlichkeit informiert werde. Er unter-

Gov discovered breach on 8 May

BfV makes clear it's an attack, not a glitch

Adversary uses common methods, making attribution harder

Remarkable: the BfV (Federal Office for the Protection of the Constitution) received information about the Parliament intrusion (C2 infrastructure and malware) from "a company that worked for another country." That country authorised the notification of the German intelligence agency.

What company and what country is unclear.

streicht, dass dieses Vertrauensverhältnis Grundvoraussetzung für die Arbeit des BSI sei. Die Pressemeldungen stimmten zudem in Teilen nicht. So träfen beispielsweise die Nachrichten, dass es sich um einen DDoS-Angriff handele, nicht zu. Er führt ergänzend aus, dass mit Informationen zu Cyberangriffen auf Firmen und Behörden auch deshalb vertraulich umgegangen werde, damit diese nicht durch Presseveröffentlichungen zusätzliche Schäden erleiden würden und zusätzlich der Angreifer gewarnt werde.

Bezüglich der Frage nach den vorhandenen Ressourcen teilt er mit, dass es im BSI etwa15 Personen mit Expertise für solche Analysen gäbe, die für den Schutz des Regierungsnetzes eingesetzt würden. Aus Erfahrung in ähnlich gelagerten Fällen gehe er davon aus, dass die Bearbeitung von Angriffen dieser Qualität über Wochen, wenn nicht Monate andauerten. Deshalb habe das BSI auch eine Fachfirma, die auch unter der Geheimschutzbetreuung stehe, hinzugezogen. Dabei sei darauf geachtet worden, dass diese Firma kompetent und auch vertrauenswürdig sei, um das Thema nationale Sicherheit ausreichend zu berücksichtigen. Es gäbe Firmen im BSI - Umfeld, die sich durch Kompetenz sowie Geheimschutzbetreuung auswiesen, mit denen das BSI insbesondere aus Ressourcengründen aber auch in Bündelung von Fachkompetenz bei Cyberangriffen außerhalb der Bundesverwaltung zusammenarbeite.

Anschließend beantwortet **Herr Hange (BSI)** die Frage von Abg. Klingbeil und teilt mit, dass nach momentanem Stand der Untersuchungen noch nicht festgestellt werden könne, wann der Ersteinbruch erfolgt sei. Aufgrund der Art der Angriffe könne gesagt werden, dass es sich um einen sogenannten APT-Angriff (advanced persistent threat) handele. Dieser verlaufe mehrstufig. Das BSI gehe davon aus, dass solche Angriffe bis zu 70 Tage in Anspruch nehmen, um ein Netz komplett zu durchdringen und damit schrittweise zu übernehmen. Habe sich der Angreifer im Netz schließlich festgesetzt, könne er sich offen bewegen, weil er dann wisse, dass er hochwahrscheinlich nicht entfernt werden könne.

Zur Frage hinsichtlich der Sicherheit teilt **Herr Hange (BSI)** mit, dass versucht werde, alle Übergänge, an denen Informationen abfließen könnten, zu kontrollieren und ggf. zu blockieren. Dabei werde jeder Schritt mit der Bundestagsverwaltung abgestimmt. Durch Maßnahmen wie dem Herunterfahren von Systemen würde versucht, für den Angreifer Ansatzpunkte abzubauen. Weiter führt **Herr Hange (BSI)** aus, dass das BSI alle Maßnahmen und Funde dokumentiere, um die Analyse auch für die IT-Experten des Bundestages nachvollziehbar und transparent zu machen.

Auch an der Täterfeststellung werde im Rahmen der technischen Analyse gearbeitet, was seiner Ansicht nach grundsätzlich schwierig sei, da es selbst in der professionell arbeitenden kriminellen Szene Verschleierungstechniken gäbe. Zunächst gehe es darum zu ermitteln, was genau geschehen sei und in welchen Systemen sich der Angreifer befinde. Wenn Endsysteme mit sensiblen Informationen infiziert seien, würden diese bereinigt, um den Export von Daten zu verhindern.

Herr Hange (BSI) führt weiter aus, dass auch die Übergänge der Bundestagsverwaltung und der Fraktionen in die Untersuchungen einbezogen werden müssten, um das Übergreifen von Schadprogrammen in den Griff zu bekommen. Er teilt weiter mit, dass nach dem Stand der Untersuchungen insbesondere der zentrale Verzeichnisdienst übernommen worden sei. Somit habe der Angreifer prinzipiell Zugriff auf alle Zugangsdaten der Fraktionen, Abgeordneten und Bundestagsmitarbeiter, die von diesem Verzeichnisdienst erfasst seien.

Zur Frage, wie eine solche Übernahme passieren könne, stellt **Herr Hange (BSI)** dar, dass für professionelle Angreifer mit tiefgreifenden Kenntnissen der Software-Systeme die Möglichkeit bestünde, noch unbekannte Schwachstellen zu entdecken und zu missbrauchen. Selbst sehr gute Software enthalte immer noch 0,7 Promille Fehler. Das Geschäft mit dem Handeln von Schwachstellen sowie Schadprogrammen verspreche viel Geld, so dass es nicht erstaunlich sei, dass Hackergruppen inzwischen auch ihre Dienste für Cyberangriffe im Internet anbieten würden. Unter Wahrung aller Vertraulichkeitsaspekte sei es sehr wichtig, schnell zu erkennen, was passiere, um die Angriffsmethodik aufzudecken, den Export von Informationen zu unterbinden und dann eine Neuaufsetzung des Systems anzugehen. Jeder dieser Schritte werde selbstverständlich mit der Bundestagsverwaltung abgesprochen.

Die **Vorsitzende** stellt die Frage, ob die Hinweise zuträfen, dass in den besonders sensiblen Bereichen wie NSA-Ausschuss, Innenausschuss oder der PKGR ein Einbruch stattgefunden habe und welche Maßnahmen dort getroffen worden seien, um Datenabflüsse zu verhindern.

Abg. Lemke stellt eine Frage zu den Ausführungen von Herrn Möhlmann (RL IT 5) zum zeitlichen Ab-

BSI has only 15 people who are qualified to investigate such high-end breaches. They are working in shifts, including on the weekends.

Attribution is hard, BSI emphasises.

BSI sees the Parliament breach as an APT. Such breaches usually take 70 days to penetrate a network, head of BSI reports (curious statement)

lauf der Information vom Bundesamt für Verfassungsschutz und dem BSI. Hier interessiere insbesondere, wer, wann, wen, worüber informiert habe. Sie fragt Herrn Hange (BSI), ob das BSI vom Verfassungsschutz informiert worden sei, unabhängig von der Information durch die Bundestagsverwaltung.

Abg. Binding fragt, auf welchen Rechnern oder Systemen Administratorrechte erlangt worden seien, um einen Eindruck zu gewinnen, welche Reichweite das Problem habe und welche Möglichkeiten dem Angreifer im System eröffnet würden.

Abg. Lemke stellt die Frage, ob es aus Sicht des BSI sinnvoll sei, die Speicherfristen der Protokolldaten wieder zu verlängern und welcher Zeitraum ggf. hier für sinnvoll erachtet würde. Weiter fragt sie, ob die Speicherung von IP-Adressen, die im Zuge der Vorratsdatenspeicherung auch diskutiert werde, eine Möglichkeit sei, die Täter zu entdecken. Zudem regt sie an, das Bundesamt für Verfassungsschutz in die IuK-Kommission einzuladen.

Abg. Dr. Sitte stellt fest, dass der Bundestag die Federführung bei der Untersuchung des Angriffes haben müsse. Sie stellt weiterhin die Frage, ob aktuell die Lückenschließung oder die Analyse des Angriffes im Vordergrund stünde. In diesem Zusammenhang möchte sie wissen, ob in diesem Fall schon jemand Anzeige erstattet habe. Des Weiteren bittet sie um Erläuterung, mit welcher personellen Ausstattung, insbesondere unter Beteiligung der externen Firma, in Zukunft vorgegangen werden solle, ob die sofortige Abschaltung aller Ressourcen diskutiert worden sei, warum dieses unterlassen worden sei und welche Konsequenzen es für den Neuaufbau habe.

Abg. Kaster merkt an, dass er Verständnis dafür habe, wie enhond des Sachstandes mit der Kommunikation umgegangen worden sei. Er bitte jedoch darum, auch in dieser Phase dem Informationsbedürfnis der Abgeordneten nachzukommen.

Die **Vorsitzende** bittet Herrn Hange (BSI) um Beantwortung der Fragen.

Herr Hange (BSI) teilt mit, dass dies nicht der erste Fall sei, der gemeinsam mit der genannten Firma bearbeitet werde. Erkennbar seien bereits gewisse Angriffsstrukturen und es sei daher zielführend, versierte Fachkräfte – d. h. IT-Forensiker – damit zu betrauen. Er betont noch einmal, dass es unverzichtbar sei, die hochqualifizierten Experten seitens des BSI zu beteiligen. Dies sei umso schwieriger, als der Analyseprozess durchaus mehrere Wochen andauern könne. Die personelle Ausstattung des BSI in diesem Umfeld betrage etwa 15 Fachleute sowie Ressourcen aus der unterstützenden Firma, die – wenn der Bundestag das wünsche – zur Verfügung stünden.

Abg. Lemke möchte wissen, ob die 15 Fachleute zeitgleich arbeiten würden.

Herr Hange (BSI) teilt mit, dass dies nicht der erste Fall sei und bei Untersuchungen vor Ort Schichtwechsel vorgenommen würden. Die erste Mannschaft habe am letzten Wochenende gearbeitet. Danach seien einige Mitarbeiter aus dem verlängerten Wochenende zurückgeholt worden, die dann in Bonn weiter gearbeitet hätten. Er weist nochmals darauf hin, dass er auch den Schutz des Regierungsnetzes nicht völlig vernachlässigen könne. Er stellt klar, dass in Absprache mit dem Deutschen Bundestag alles getan werde, um seitens des BSI die Personen mit dem größtmöglichen Erfahrungsschatz in diesem Umfeld mit der Aufgabe zu betrauen. Er informiert, dass der externe Partner in diesem Fall die Firma BFK sei und dass bei Bedarf auch Mitarbeiter der Firma Telekom, die ebenfalls über ein Team mit ähnlichen Kenntnissen verfügten, hinzugezogen werden könnten. Im Augenblick sehe er jedoch keine Notwendigkeit hierfür.

Confirms BFK

Telekom apparently has an APT research team, but BSI did not consider it necessary to request that team. This almost sounds as if Telekom is better equipped to deal with these challenge than BSI. Hard to believe.

Herr Hange (BSI) betont noch einmal, dass es nur durch die Erkenntnisse aus der Analyse möglich sein werde, dem Angreifer den Weg zu verbauen. Die Angreifer hätten sich bereits tief in den Systemen verankert und würden sich inzwischen sogar recht auffällig bewegen, da sie aus Erfahrung nicht mehr fürchten müssten, mit einfachen Mitteln entfernt werden zu können.

Grundsätzlich sei ein Angreifer in einer besseren Position als der Verteidiger, da er den Angriffspunkt selbst bestimmen könne. Weiter führt er aus, dass der gesamte Vorgang dokumentiert werde. Im konkreten Fall sei der Bundestag vom Bundesamt für Verfassungsschutz angerufen worden und es sei mitgeteilt worden, dass auch das BSI informiert werde, da prinzipiell nicht auszuschließen sei, dass auch Regierungsstellen betroffen seien. Im weiteren Verlauf zwischen Bundestag und BSI sei entschieden worden, dass zwei Mitarbeiter des BSI am Freitag, dem 15.5.2015 im Bundestag in einem Erstgespräch über die möglichen weiteren Schritte informierten. Kurzfristig sei aufgrund der Besprechung dann beschlossen worden, unverzüglich am Wochenende mit der tiefer gehenden Analyse zu beginnen.

In principle offender is in better position than defender

Abg. Lemke fragt weiter nach den vom Verfassungsschutz festgestellten Auffälligkeiten.

Herr Hange (BSI) teilt mit, dass ein Server auffällig geworden sei, welcher auf einer Liste als kritisch eingestufter Server stehe. Die Rückmeldemöglichkeiten dieser bekannten Server würden vom BSI unterbunden. Im technischen Bereich sei dies ein transparentes Verfahren ohne nachrichtendienstliche Hintergründe. Er führt aus, dass es einen weltweiten CERT-Verbund zum Austausch von genau solchen kritischen Hinweisen ohne nachrichtendienstlichen Hintergrund gebe. Ein Informationsaustausch zwischen dem BSI und dem Bundesamt für Verfassungsschutz erfolge nur dann, wenn der Verdacht von Cyberspionage fremder Staaten gegeben sei.

Abg. Dr. Brandl erklärt, dass er zwar Verständnis für die Nachfrage zum Verfassungsschutz habe, es aber genau Aufgabe des Verfassungsschutzes sei, elektronische Angriffe mit möglicherweise nachrichtendienstlichem Hintergrund auf die Bundesrepublik festzustellen und die betroffenen Behörden zu informieren. Er verdeutlicht seine Ansicht, dass der Verfassungsschutz auch nach einem Hinweis eines ausländischen Anbieters – sei es Staat, Firma oder CERT – unverzüglich zu informieren habe, wenn aus dem Bereich eines Regierungsnetzes ein Zugriff auf einen kompromittierten Server festgestellt werde. Er betont, dass er positiv zur Kenntnis nehme, dass diese Meldewege funktionierten.

Abg. Klingbeil fragt nach, ob die Art und Weise der Angriffe dem BSI als Muster bekannt seien und es hierfür bereits bekannte Akteure gäbe. Und ob es sich hierbei um Geheimdienste oder Unternehmen handele, die von Staaten für solche Angriffe beauftragt werden würden.

Herr Hange (BSI) stellt dar, dass es sich bisheriger Kenntnis nach um Gruppierungen handele, die nicht das BSI beobachte. Wenn technische Analysen Rückschlüsse auf Tätergruppen zulassen, sei es Aufgabe des Cyberabwehrzentrums, beim BfV, BKA oder BND nachzufragen, ob mehr zu diesen Gruppierungen bekannt sei. Er erklärt, dass die Einschätzung der Fähigkeiten des Angreifers auch entscheidend dafür sei, um die notwendige Abwehr einzuordnen. Er macht noch einmal deutlich, dass ein Angriff in dieser Form nicht zum ersten Mal erfolge und die Weitergabe von Hinweisen an die betroffenen Firmen oder Behörden in festgelegter Weise erfolge.

Abg. Klingbeil fragt nach, ob das Muster des Angriffes als Mittel von Nachrichtendiensten bekannt sei.

Herr Hange (BSI) bejaht, dass das Muster des Angriffes zwar bekannt sei, es aber dennoch nach jetzigem Untersuchungsstand nicht eindeutig einzuordnen sei, ob es von den vermuteten Akteuren durchgeführt oder einfach kopiert worden sei. Es sei in letzter Zeit auch festgestellt worden, dass einfachere Angriffsmuster, die bislang bestimmten Ländern und Gruppierungen zugeordnet werden konnten, nachgeahmt würden. Das BSI beschäftige sich in seiner Schutzfunktion mit der Bekämpfung des Angriffsmusters, mit der Täterermittlung nur im Rahmen technischer Analysen. Die Täterermittlung sei Aufgabe der dafür zuständigen Sicherheitsbehörden.

BSI reports that adversaries have started imitating common features of other known adversaries, basically: false flag operations on the rise.

Herr Häger (BSI) ergänzt, dass es sich um ein generisches Angriffsmuster handele und damit nach Stand der Untersuchungen einer konkreten Tätergruppe noch nicht zugeordnet werden könne. Er erklärt, dass nach jetzigem Erkenntnisstand der Täter mit seinem Schadprogramm in das Netz gelange, dort seine Rechte ausweite und den Verzeichnisdienst übernommen habe, um dann auf beliebige Systeme Zugriff zu haben. Dieses entspreche einem hochwertigen APT-Angriffsmuster.

Die Vorsitzende erläutert, dass entsprechend der Beschlusslage die Obleute am letzten Mittwoch durch das Sekretariat über ihre Entscheidung zur Verlängerung der Speicherfrist von ursprünglich sieben Tagen auf maximal drei Monate informiert worden seien. Sie merkt weiter an, dass es ihrer Einschätzung nach erst am Ende dieses ganzen Prozesses zu einer erneuten Diskussion über die Speicherfristen kommen könne. Sie bedankt sich im Namen der ganzen Kommission für die erhaltenen Informationen und schlägt eine erneute Sitzung für die kommende Sitzungswoche vor.

Sie merkt an, dass am Nachmittag über den Ältestenrat die Fraktionen in geeigneter Weise über den in der IuK-Kommission vorgetragenen Sachverhalt informiert würden. Gegebenenfalls sei je nach Entscheidung des Ältestenrates noch in dieser Sitzungswoche eine Obleuterunde einzuberufen. Sie gehe davon aus, dass die Obleute der IuK-Kommission auch in den kommenden Nichtsitzungswochen in geeigneter Form vom Sekretariat über aktuelle Entwicklungen informiert würden. Sie werde sich mit dem Präsidenten über eine abgestimmte Information für alle Kolleginnen und Kollegen ins Benehmen setzen.

Die Abg. Lemke stimmt der Vorsitzenden in vollem Umfang zu. Sie bekräftigt, dass gerade in Anbe-

tracht der zwei Nichtsitzungswochen eine allgemeine Information für alle Mitglieder erforderlich scheine.

Die **Vorsitzende** stellt fest, dass sich die IuK-Kommission über die kurzfristig erforderlichen Kommunikationswege einig sei. Da auch zum Punkt Verschiedenes keine weiteren Wortmeldungen vorliegen, bedankt sich die **Vorsitzende** bei den Vortragenden und schließt die Sitzung.

Schluss der Sitzung: 9:10 Uhr

Petra Pau, MdB

Vorsitzende